

CLAIMS

What is claimed is:

- 1 1. A method for providing a cryptographic service utilizing a server on a
2 network, comprising:
3 (a) identifying a client utilizing the network;
4 (b) establishing a first key;
5 (c) generating a tunnel on the network;
6 (d) receiving information at the server from the client utilizing the tunnel,
7 wherein the information is encrypted by the client using the first key; and
8 (e) performing work at the server.
- 1 2. A method as recited in claim 1, wherein a second key is encrypted by the
2 client using the first key, and further comprising receiving the second key at
3 the server.
- 1 3. A method as recited in claim 2, wherein the second key comprises at least
2 one parameter for the work performed by the server.
- 1 4. A method as recited in claim 1, wherein the work includes cryptographic
2 services.
- 1 5. A method as recited in claim 1, wherein the work includes modular
2 exponentiation.
- 1 6. A method as recited in claim 1, further comprising the step of transmitting
2 work results to the client.
- 1 7. A method as recited in claim 6, further comprising the step of encrypting the
2 work results utilizing the first key.

05

- 1 8. A method as recited in claim 6, wherein the work results are transmitted to a
2 third party.
- 1 9. A method as recited in claim 1, further comprising the step of charging a fee
2 for the work performed by the server.
- 1 10. A method as recited in claim 9, wherein the fee is charged to the client.
- 1 11. A method as recited in claim 1, wherein the first key comprises an encryption
2 key for a symmetric cipher.
- 1 12. A method as recited in claim 1, wherein the first key comprises an encryption
2 key for an asymmetric cipher.
- 1 13. A computer program embodied on a computer readable medium for
2 providing a cryptographic service utilizing a server on a network,
3 comprising:
4 (a) a code segment for identifying a client utilizing the network;
5 (b) a code segment for establishing a first key;
6 (c) a code segment for generating a tunnel on the network;
7 (d) a code segment for receiving information at the server from the client
8 utilizing the tunnel, wherein the information is encrypted by the client using
9 the first key; and
10 (e) a code segment for performing work at the server.
- 1 14. A computer program as recited in claim 13, wherein a second key is
2 encrypted by the client using the first key, and further comprising a code
3 segment for receiving the second key at the server.

[illegible]

- 1 15. A computer program as recited in claim 14, wherein the second key
2 comprises at least one parameter for the work performed by the server.
- 1 16. A computer program as recited in claim 13, wherein the work includes
2 cryptographic services.
- 1 17. A computer program as recited in claim 13, wherein the work includes
2 modular exponentiation.
- 1 18. A computer program as recited in claim 13, further comprising a code
2 segment that transmits work results to the client.
- 1 19. A computer program as recited in claim 18, further comprising a code
2 segment that encrypts the work results utilizing the first key.
- 1 20. A system for providing a cryptographic service utilizing a server on a
2 network, comprising:
3 (a) logic for identifying a client utilizing the network;
4 (b) logic for establishing a first key;
5 (c) logic for generating a tunnel on the network;
6 (d) logic for receiving information at the server from the client utilizing the
7 tunnel, wherein the information is encrypted by the client using the first key;
8 and
9 (e) logic for performing work at the server.
- 1 21. A method as recited in claim 3, wherein a message or a cyphertext comprises
2 a second parameter for the work performed by the server.
- 1 22. A method as recited in claim 21, wherein the message or cyphertext has been
2 blinded by the user before transmittal to the server.